Permutationen[1]

Die symmetrische Gruppe

Eine **Permutation** ist eine bijektive Abbildung einer Menge M auf sich selbst. Die Permutationen von M bilden eine Gruppe $\mathrm{Abb}(M, M)$.

Diese Gruppe ist (zumindest in der diskreten Mathematik, zu der wir hier auch die Kryptologie zählen dürfen) von besonderem Interesse, wenn die Menge M endlich ist. Auf die Natur der Elemente kommt es hierbei meist nicht an. (Wer will, mag dieses Statement in die präzise mathematische Aussage: „Eine bijektive Abbildung zwischen zwei Mengen M und N induziert einen Gruppenisomorphismus zwischen $\mathrm{Abb}(M, M)$ und $\mathrm{Abb}(N, N)$“ übersetzen.) Daher wird die Menge M oft einfach als die Menge der natürlichen Zahlen $\{1, \ldots, n\}$ angenommen. Die Gruppe $\mathrm{Abb}(M, M)$ wird dann auch als $\mathcal{S}_n$ bezeichnet und **symmetrische Gruppe** der Ordnung n genannt.

Satz 1 *Die symmetrische Gruppe der Ordnung n hat $n!$ Elemente; als Formel ausgedrückt:*

$$\#\mathcal{S}_n = n!.$$

Beweis. Eine Permutation π ist durch ihre Werte für die Argumente $1, \ldots, n$ eindeutig festgelegt. Für $\pi 1$ gibt es n Möglichkeiten, für $\pi 2$ dann noch $n-1$, $\ldots$, für $\pi(n-1)$ noch zwei und für πn schließlich noch eine. Das macht zusammen $n!$. $\diamond$

(Die Punkte „$\ldots$“ werden abkürzend für einen Beweis durch vollständige Induktion verwendet.)

Beschreibung von Permutationen

Eine Permutation π der Menge $\{1, \ldots, n\}$ wird oft durch ihre Wertetafel ausgedrückt, die man in Zeilenform schreibt:

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \pi 1 & \pi 2 & \ldots & \pi n \end{pmatrix}.$$

Selbstverständlich kann man diese Schreibweise auch auf andere Grundmengen M übertragen; nimmt man als Grundmenge etwa $\{\mathrm{A}, \ldots, \mathrm{Z}\}$, also das in der klassischen Kryptologie meistens verwendete Alphabet, so ist eine Permutation nichts anderes als eine monoalphabetische Substitution σ und wird ebenfalls in der Form

$$\begin{pmatrix} A & \ldots & Z \\ \sigma A & \ldots & \sigma Z \end{pmatrix}$$

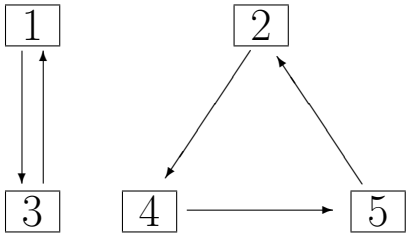
[1] Klaus Pommerening, Kryptologie; 7. Januar 2008, letzte Änderung: 23. Januar 2008

notiert, oft ohne die Klammern; unter jeden Buchstaben wird also sein Bild bei der Verschlüsselung geschrieben.

Eine andere Beschreibung einer Permutation π ist die **Zykel-Darstellung**. Diese wird erst an einem Beispiel mit $n = 5$ erläutert: Die Permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$$

kann man zunächst grafisch darstellen:



und dieser Graph wird vollständig beschrieben durch die Zahlenanordnung

$$(1\,3)(2\,4\,5).$$

Das bedeutet: Jede Klammer beschreibt einen „Zykel“ – man beginnt mit einem beliebigen Element, schreibt daneben sein Bild, dann dessen Bild usw., bis man wieder auf das Ausgangselement stößt. Danach nimmt man ein noch nicht aufgeschriebenes Element, sofern noch eines übrig ist, und verfährt mit diesem genau so usw., bis alle Elemente in der Zykel-Darstellung vorkommen. Fixpunkte der Permutation ergeben Zykel der Länge 1. Die allgemeine Formel ist

$$(a_1, \pi a_1, \ldots, \pi^{k_1-1} a_1) \cdots (a_i, \pi a_i, \ldots, \pi^{k_i-1} a_i) \cdots ,$$

wobei k_i die kleinste natürliche Zahl ≥ 1 ist mit $\pi^{k_i} a_i = a_i$.

Damit ist auch bewiesen:

Satz 2 *Jede Permutation einer endlichen Menge lässt sich in disjunkte Zykel zerlegen. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Zykel und die zyklische Vertauschung der Elemente in jedem Zykel.*

Gruppentheoretische Deutung

Ein Zykel kann selbst als Permutation gedeutet werden: die im Zykel stehenden Elemente werden in der angegebenen Reihenfolge zyklisch vertauscht, die anderen werden festgelassen.

Beispiel: Der Zykel $(2\,4\,5)$ in $\mathcal{S}_5$ entspricht also der Permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix} \quad \text{oder in Zykeldarstellung} \quad (1)(2\,4\,5)(3).$$

Der Zykel (i) in $\mathcal{S}_n$ entspricht der identischen Abbildung, egal welches $i = 1, \ldots, n$ man wählt. Identifiziert man Zykel mit den durch sie beschriebenen Permutationen, so sieht man sofort:

Hilfssatz 1 *Disjunkte Zykel sind vertauschbar, kommutieren also als Elemente der Gruppe $\mathcal{S}_n$.*

Das Nebeneinanderschreiben der Zykel in der Zykelzerlegung einer Permutation entspricht gerade dem Produkt der entsprechenden Permutationen in $\mathcal{S}_n$. Man kann also Satz 2 auch so ausdrücken:

Korollar 1 *Jede Permutation lässt sich eindeutig bis auf die Reihenfolge als Produkt von disjunkten Zykeln schreiben.*

Ist r_k die Anzahl der Zykel der Länge k einer Permutation $\pi \in \mathcal{S}_n$, so ist

$$n \cdot r_n + \cdots + 1 \cdot r_1 = n.$$

Eine endliche Folge $[s_1 s_2 \ldots s_m]$ von natürlichen Zahlen mit $s_1 \geq \ldots \geq s_m \geq 1$ heißt **Partition** von n, wenn $n = s_1 + \cdots + s_m$. Schreibt man die Zykellängen einer Permutation $\pi \in \mathcal{S}_n$ der Größe nach geordnet in dieser Form auf – jede der Längen mit der Vielfachheit, in der sie vorkommt – so erhält man also eine Partition von n. Diese heißt der **(Zykel-) Typ** von π.

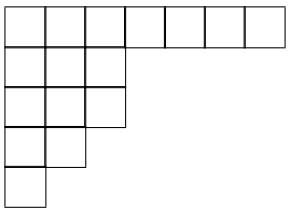
Beispiel: Der Zykeltyp von

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} = (1\,3)(2\,4\,5)$$

ist

$$[3\,2].$$

Veranschaulicht werden Partitionen oft duch YOUNG**-Diagramme**. Zur Partition $[s_1 s_2 \ldots s_m]$ von n wird das YOUNG-Diagramm gebildet, indem man im m Zeilen untereinander linksbündig jeweils s_i Kästchen anordnet. Zur Partition [7 3 3 2 1] von 16 gehört das Diagramm



(Die definierende Bedingung für ein YOUNG-Diagramm ist, dass keine Zeile länger als die darüber stehende ist.)

Konjugierte Permutationen

Seien $\pi, \rho \in \mathcal{S}_n$; gesucht ist der Zusammenhang der Zykeldarstellung von π und der der konjugierten Permutation $\rho\pi\rho^{-1}$. Betrachten wir zunächst den Fall, dass π nur ein Zykel ist,

$$\pi = (a_1 \ \dots \ a_k),$$

also $\pi a_i = a_{i+1 \bmod k}$ für $i = 1, \dots, k$, während alle anderen Elemente Fixpunkte sind. Dann ist für $b_i = \rho a_i$

$$\rho\pi\rho^{-1} b_i = \rho\pi a_i = \rho a_{i+1 \bmod k} = b_{i+1 \bmod k}.$$

Also ist

$$\rho\pi\rho^{-1} = (b_1 \ \dots \ b_k).$$

Daher ist auch $\rho\pi\rho^{-1}$ ein Zykel der Länge k.

Die Konjugation mit ρ ist ein innerer Automorphismus der Gruppe $\mathcal{S}_n$, d. h., $\rho(\pi_1\pi_2)\rho^{-1} = (\rho\pi_1\rho^{-1})(\rho\pi_2\rho^{-1})$. Daher kann man im allgemeinen Fall die Zykel von π einzeln mit ρ konjugieren und erhält als Ergebnis den ersten Teil des folgenden Satzes:

Hauptsatz 1 (i) *Für zwei Permutationen $\pi, \rho \in \mathcal{S}_n$ erhält man die Zykel-Zerlegung der konjugierten Permutation $\rho\pi\rho^{-1}$ aus der von π, indem man in jeden Zykel $(a_1 \ \dots \ a_k)$ von π durch den Zykel $(\rho a_1 \ \dots \ \rho a_k)$ ersetzt.*

(ii) *Zwei Permutationen einer endlichen Menge sind genau dann zueinander konjugiert, wenn sie den gleichen Zykel-Typ besitzen.*

Mit anderen Worten: Die Konjugationsklassen der symmetrischen Gruppe $\mathcal{S}_n$ entsprechen auf natürliche Weise den Partitionen von n bzw. den YOUNG-Diagrammen, die man aus n Kästchen bilden kann.

Beweis. Nur noch die Rückrichtung der zweiten Aussage ist zu beweisen. Seien dazu $\sigma, \tau \in \mathcal{S}_n$ vom gleichen Zykel-Typ. Schreibt man nun die Zykelzerlegungen von σ und τ so untereinander, dass jeweils Zykel gleicher Länge untereinander stehen, so kann man eine Permutation ρ mit $\rho\sigma\rho^{-1} = \tau$ ablesen: Sie bildet jedes Element auf das darunter stehende ab. $\diamond$

Dieser Satz, so einfach er auch ist, bildet eine wesentliche Grundlage für die Kryptoanalyse der Verschlüsselungsmaschine Enigma und wurde daher auch schon mal „der Satz, der den zweiten Weltkrieg gewann“ genannt; das ist natürlich übertrieben, aber eine wesentliche Beschleunigung des Kriegsendes wurde dadurch ziemlich sicher bewirkt.

Übungsaufgabe. Beschreibe zu $\sigma, \tau \in \mathcal{S}_n$ die Gesamtheit aller Lösungen ρ von $\rho\sigma\rho^{-1} = \tau$.

Transpositionen

Eine **Transposition** ist ein Zykel der Länge 2, d. h., eine Permutation, die zwei Elemente vertauscht und die übrigen festlässt. An der Formel

$$(a_1\ a_2\ \ldots\ a_k) = (a_1\ a_k)\cdots(a_1\ a_3)(a_1\ a_2)$$

sieht man:

Hilfssatz 2 *Jeder Zykel der Länge k lasst sich als Produkt von $k-1$ Transpositionen schreiben.*

Und damit folgt aus Satz 2 weiter:

Korollar 2 *Jede Permutation π lässt sich als Produkt von $n-r$ Transpositionen schreiben, wobei r die Zahl der Zykel mit mehr als einem Element in der Zykelzerlegung von π ist.*

Da die Transpositionen nicht disjunkt sind, sind sie im allgemeinen nicht vertauschbar, und die Zerlegung in Transpositionen ist auch nicht eindeutig. Nicht einmal die Anzahl der Transpositionen ist eindeutig; immerhin gilt aber:

Satz 3 *Schreibt man eine Permutation $\pi \in \mathcal{S}_n$ auf verschiedene Weise als Produkt von Transpositionen, so ist deren Anzahl entweder stets gerade oder stets ungerade.*

Beweis. Sei $\pi = \tau_1 \cdots \tau_s$ mit Transpositionen τ_i. Andererseits sei $\pi = \zeta_1 \cdots \zeta_r$ die Zerlegung in disjunkte Zykel (vollständig, also einschließlich aller Zykel der Länge 1). Multipliziert man nun π von links mit einer Transposition $\tau = (a\,b)$, so gibt es zwei Fälle:

1. Fall. a und b sind im selben Zykel enthalten. Dann kann man, da die Zykel kommutieren, annehmen, dass dies der erste $\zeta_1 = (a_1\ \ldots\ a_k)$ ist, und $a = a_1$, $b = a_i$. Dann bewirkt $\tau\pi$

$$\begin{array}{rcl}
a_1 \overset{\pi}{\mapsto} & a_2 & \overset{\tau}{\mapsto} a_2 \\
& \vdots & \\
a_{i-1} \mapsto & a_i & \mapsto a_1 \\
a_i \mapsto & a_{i+1} & \mapsto a_{i+1} \\
& \vdots & \\
a_k \mapsto & a_1 & \mapsto a_i
\end{array}$$

Also ist $\tau\pi = (a_1\ \ldots\ a_{i-1})(a_i\ \ldots\ a_k)\zeta_2 \cdots$ (übrige Zykel unverändert).

2. Fall. a und b sind im verschiedenen Zykeln enthalten. Dann kann man annehmen, dass dies die ersten beiden $\zeta_1 = (a_1\ \ldots\ a_k)$ und $\zeta_2 = (b_1\ \ldots\ b_l)$ sind, und $a = a_1$, $b = b_1$. Dann ist $\tau\pi = (a_1\ \ldots\ a_k\, b_1\ \ldots\ b_l)\zeta_3 \cdots$.

Die Zykelzahl hat sich also um 1 erhöht oder um 1 erniedrigt, ist also $r \pm 1$. Multipliziert man nun von links mit einer weiteren Transposition, so wird die Zykelzahl zu $r+2$, r oder $r-2$. Hat man q Transpostionen von links dranmultipliziert, sind es $r + t_q$ Zykel, wobei $t_q \equiv q \pmod 2$. Das Produkt $\tau_s \cdots \tau_1 \pi$ hat also $r + t_s$ Zykel mit $t_s \equiv s \pmod 2$. Da es aber die identische Abbildung $\pi^{-1}\pi$ ist, ist $r + t_s = n$. Also ist $s \equiv n - r \pmod 2$, egal mit welcher Zerlegung in Transpositionen wir gestartet sind. $\diamond$

Die alternierende Gruppe

Ordnet man jeder Permutation in $\mathcal{S}_n$ die Parität der Anzahl der Transpositionen einer beliebigen Zerlegung zu, so hat man nach dem vorigen Abschnitt eine wohldefinierte Funktion

$$\operatorname{sgn} : \mathcal{S}_n \longrightarrow \mathbb{F}_2,$$

von der man leicht sieht, dass sie ein Gruppenhomomorphismus in die additive Gruppe ist. Der Kern heißt die **alternierende Gruppe** der Ordnung n und wird mit $\mathbf{A}_n$ bezeichnet. Die Elemente von $\mathbf{A}_n$, also die Permutationen, die sich in eine gerade Anzahl von Transpositionen zerlegen lassen, heißen **gerade** Permutationen, die anderen **ungerade**. $\mathbf{A}_n$ ist ein Normalteiler vom Index 2 in $\mathcal{S}_n$ und hat daher $n!/2$ Elemente.

Involutionen

Eine Permutation heißt **Involution**, wenn sie als Gruppenelement in $\mathcal{S}_n$ die Ordnung 2 hat, oder alternativ, wenn ihre Zykel-Zerlegung nur aus Transpositionen (und Fixpunkten) besteht. Eine Involution heißt **echt**, wenn sie keine Fixpunkte hat. Das ist natürlich nur möglich, wenn n gerade ist. Eine echte Involution ist also ein Produkt von $n/2$ disjunkten Zweierzykeln.

Eine Aufgabe, die bei der Berechnung der Größe des Schlüsselraums der Enigma auftritt, ist die Bestimmung der Anzahl der Involutionen in der symmetrischen Gruppe $\mathcal{S}_n$ mit genau k Zweierzykeln, wobei $0 \leq 2k \leq n$. Sie ist gleich der Anzahl $d(n,k)$ der Möglichkeiten, k Paare aus n Elementen zu wählen (wobei es innerhalb der Paare nicht auf die Reihenfolge ankommt).

Wahl von	**Möglichk.**	**Wahl v.**	**Möglichkeiten**
1. Element:	n		
1. Partner:	$n-1$	1. Paar:	$n(n-1)/2$
2. Element:	$n-2$		
2. Partner:	$n-3$	2. Paar:	$(n-2)(n-3)/2$
...	...	...	...
k. Element:	$n-2(k-1)$		
k. Partner:	$n-2(k-1)-1$	k. Paar:	$(n-2k+2)(n-2k+1)/2$

Insgesamt ergibt das mit Berücksichtigung der Reihenfolge

$$\frac{n(n-1)\cdots(n-2k+2)(n-2k+1)}{2^k} = \frac{n!}{(n-2k)!\cdot 2^k}$$

Möglichkeiten. Davon sind, wenn man nun die Reihenfolge außer Acht lässt, jeweils $k!$ identisch. Damit ist gezeigt:

Satz 4 *Die Anzahl der Involutionen in der symmetrischen Gruppe $\mathcal{S}_n$ mit genau k Zweierzykeln ist*

$$d(n,k) = \frac{n!}{2^k k!(n-2k)!} \quad \textit{für } 0 \le 2k \le n.$$

Beispiel. Im Falle der Wehrmachts-Enigma ist $n = 26$ und $k = 10$, die Zahl der möglichen Involutionen also

$$\frac{26!}{2^{10}\cdot 10!\cdot 6!} = 150738274937250.$$

Produkte echter Involutionen

Bei der Kryptoanalyse der Enigma spielen Produkte von jeweils zwei echten Involutionen σ und τ eine Rolle. Sei $(a\,b)$ ein Zykel von τ. Falls $(a\,b)$ auch Zykel von σ ist, läßt $\sigma\tau$ die beiden Elemente a und b fix, hat also die beiden Einerzykel (a) und (b).

Im allgemeinen Fall findet man von einem beliebigen Element a_1 ausgehend eine Kette $a_1, a_2, a_3, \ldots, a_{2k}$, so dass

$$\begin{aligned} \tau = &\quad (a_1\,a_2)(a_3\,a_4)\cdots(a_{2k-1}\,a_{2k}) && \text{mal weitere Zweierzykel,}\\ \sigma = &\quad (a_2\,a_3)(a_4\,a_5)\cdots(a_{2k}\,a_1) && \text{mal weitere Zweierzykel.} \end{aligned}$$

Im Produkt $\sigma\tau$ werden daraus die beiden Zykel

$$(a_1\,a_3\,\ldots\,a_{2k-1})(a_{2k}\,\ldots\,a_4\,a_2)$$

der Länge k. Insbesondere treten alle Zykellängen in gerader Anzahl auf, der Zykel-Typ ist **paarig**.

Hauptsatz 2 [Rejewski] *Eine Permutation ist genau dann das Produkt zweier echter Involutionen, wenn ihr Zykel-Typ paarig ist.*

Beweis. Die Umkehrung beweist man, in dem man zu einer Permutation π von paarigem Zykel-Typ Lösungen σ, τ der Gleichung $\sigma\tau = \pi$ angibt.

Im einfachsten Fall, wo π nur aus zwei Zykeln gleicher Länge besteht, also

$$\pi = (p_1\,p_2\,\ldots\,p_k)(q_1\,q_2\,\ldots\,q_k),$$

ist eine Lösung offenbar durch

$$\begin{aligned}\tau &= (p_1\ q_k)(p_2\ q_{k-1})\cdots(p_k\ q_1),\\ \sigma &= (p_2\ q_k)(p_3\ q_{k-1})\cdots(p_1\ q_1)\end{aligned}$$

gegeben.

Im allgemeinen Fall konstruiert man analog die Lösung getrennt für je ein paar gleichlanger Zykel. $\diamond$

Man erhält eine Lösung also nach folgendem Verfahren: Man schreibt Zykel gleicher Länge untereinander, den unteren in umgekehrter Reihenfolge. Dann liest man die Zweierzykel von τ ab, indem je zwei untereinanderstehende Elemente paart, die von σ, indem man jedes Element mit dem links darunter stehenden paart.

Beispiel. Sei $\pi =$ `(D)(K)(AXT)(CGY)(BLFQVEOUM)(HJPSWIZRN)`. Dann paart man

```
(D)(AXT)(BLFQVEOUM)
(K)(YGC)(NRZIWSPJH)
```

und hat als eine Lösung von $\sigma\tau = \pi$:

$$\begin{aligned}\tau &= \texttt{(DK)(AY)(XG)(TC)(BN)(LR)(FZ)(QI)(VW)(ES)(OP)(UJ)(MH)},\\ \sigma &= \texttt{(DK)(XY)(TG)(AC)(LN)(FR)(QZ)(VI)(EW)(OS)(UP)(MJ)(BH)}.\end{aligned}$$

Man sieht auch leicht, wie alle Lösungen aussehen: Man kann den unteren Zykel jeweils zyklisch verschieben, und wenn es mehr als zwei Zykel gleicher Länge gibt, hat man noch alle möglichen Paarungen zu berücksichtigen. Die Lösung wird eindeutig, sobald zu jedem Zykelpaar ein Zweierzykel von σ oder τ festgelegt ist.

Übungsaufgabe. Der Leser möge die Formel für die Anzahl der Lösungen selbst ausarbeiten.